(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
31 décembre 2003 (31.12.2003)

PCT

(10) Numéro de publication internationale
WO 2004/002058 A3

(51) Classification internationale des brevets[7] : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR2003/001871

(22) Date de dépôt international : 18 juin 2003 (18.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/07688 19 juin 2002 (19.06.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Parc d'Activités de Gémenos, Avenue du Pic-de-Bertagne, F-13420 Gémenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **FEYT, Nathalie** [FR/FR]; 8, chemin de Raphèle, 7 lotissement l'Oliveraie, F-13780 Cuges les Pins (FR). **JOYE, Marc** [FR/FR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR).

(74) Mandataire : **AIVAZIAN, Denis**; Gemplus la Vigie, Service brevets, BP 100, F-13705 La Ciotat Cedex (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— *relative à l'identité de l'inventeur (règle 4.17.i)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii)) pour les désignations suivantes AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

[Suite sur la page suivante]

(54) **Title:** METHOD OF GENERATING ELECTRONIC KEYS FOR A PUBLIC-KEY CRYPTOGRAPHY METHOD AND A SECURE PORTABLE OBJECT USING SAID METHOD

(54) **Titre :** PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN OEUVRE LE PROCEDE

(57) **Abstract:** The invention relates to a method of generating electronic keys (d) for a public-key cryptography method using an electronic device. The inventive method comprises two separate calculation steps, namely: step A consisting in (i) calculating pairs of prime numbers (p, q), said calculation being independent of knowledge of the pair (e, l) in which e is the public exponent and l is the length of the key of the cryptography method, and (ii) storing the pairs thus obtained; and step B which is very quick and can be executed in real time by the device, consisting in calculating a key d from the results of step A and knowledge of the pair (e, l).

(57) **Abrégé :** L'invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique. Selon l'invention, le procédé comprend deux étapes de calcul dissociées. Une étape A consiste à - calculer des couples de nombres premiers (p, q), ce calcul est indépendant de la connaissance du couple (e, l) e l'exposant public et l la longueur de la clé du procédé de cryptographie et à - stocker les couples ainsi obtenus. Une étape B très rapide qui peut être exécutée en temps réel par le dispositif, consiste à calculer une clé d à partir des résultats de l'étape A et de la connaissance du couple (e, l).

WO 2004/002058 A3

— *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii)) pour toutes les désignations*
— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :
— *avec rapport de recherche internationale*

(88) Date de publication du rapport de recherche internationale: 15 avril 2004

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01871

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4 736 423 A (MATYAS STEPHEN M) 5 April 1988 (1988-04-05) column 9, line 58 -column 11, line 30	1
A	column 14, line 57 - line 59	4,7,12
Y	GANESAN R: "Yaksha: augmenting Kerberos with public key cryptography" NETWORK AND DISTRIBUTED SYSTEM SECURITY, 1995., PROCEEDINGS OF THE SYMPOSIUM ON SAN DIEGO, CA, USA 16-17 FEB. 1995, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, 16 February 1995 (1995-02-16), pages 132-143, XP010134533 ISBN: 0-8186-7027-4	1
A	page 142, right-hand column, line 11 - line 17	12

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
4 December 2003	12/12/2003
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR [redacted]01871

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	B. SCHNEIER: "APPLIED CRYPTOGRAPHY" 1996 , WILEY , NEW YORK XP002234403 page 466, paragraph 19.3 -page 469, last line	1,3,6,12
A	FR 2 811 442 A (GEMPLUS CARD INT) 11 January 2002 (2002-01-11) abstract page 2, line 21 -page 3, line 12 page 8, line 11 - line 22	2,8

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR [redacted]1871

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 4736423	A	05-04-1988	DE	3685987 D1	20-08-1992
			DE	3685987 T2	04-02-1993
			EP	0202768 A2	26-11-1986
FR 2811442	A	11-01-2002	FR	2811442 A1	11-01-2002
			AU	6922101 A	21-01-2002
			CN	1449609 T	15-10-2003
			EP	1302021 A1	16-04-2003
			WO	0205483 A1	17-01-2002

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR [redacted]1871

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, PAJ, EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
Y	US 4 736 423 A (MATYAS STEPHEN M) 5 avril 1988 (1988-04-05) colonne 9, ligne 58 -colonne 11, ligne 30	1
A	colonne 14, ligne 57 - ligne 59	4,7,12
Y	GANESAN R: "Yaksha: augmenting Kerberos with public key cryptography" NETWORK AND DISTRIBUTED SYSTEM SECURITY, 1995., PROCEEDINGS OF THE SYMPOSIUM ON SAN DIEGO, CA, USA 16-17 FEB. 1995, LOS ALAMITOS, CA, USA,IEEE COMPUT. SOC, 16 février 1995 (1995-02-16), pages 132-143, XP010134533 ISBN: 0-8186-7027-4	1
A	page 142, colonne de droite, ligne 11 - ligne 17	12

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
4 décembre 2003	12/12/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/F[redacted]/01871

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	B. SCHNEIER: "APPLIED CRYPTOGRAPHY" 1996 , WILEY , NEW YORK XP002234403 page 466, alinéa 19.3 -page 469, dernière ligne	1,3,6,12
A	FR 2 811 442 A (GEMPLUS CARD INT) 11 janvier 2002 (2002-01-11) abrégé page 2, ligne 21 -page 3, ligne 12 page 8, ligne 11 - ligne 22	2,8

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR [redacted]1871

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
US 4736423	A	05-04-1988	DE	3685987 D1	20-08-1992
			DE	3685987 T2	04-02-1993
			EP	0202768 A2	26-11-1986
FR 2811442	A	11-01-2002	FR	2811442 A1	11-01-2002
			AU	6922101 A	21-01-2002
			CN	1449609 T	15-10-2003
			EP	1302021 A1	16-04-2003
			WO	0205483 A1	17-01-2002